UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/681,203	02/21/2001	Ariel Katz	1018.126US1	5124

22971 7590 09/01/2006

MICROSOFT CORPORATION
ATTN: PATENT GROUP DOCKETING DEPARTMENT
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/681,203	KATZ ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-10,12-14,16-24 and 26-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-10,12-14,16-24 and 26-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 23 June 2006 has been noted and made of record.

2. Claims 1, 4-10, 12-14, 16-24, and 26-36 have been presented for examination.

3. Claims 2, 3, 11, and 15 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments filed 23 June 2006 have been fully considered but they are not persuasive.

5. With respect to the Applicant's allegation that *Perlman* does not teach a proxy, the Examiner directs the Applicant's attention to MPEP § 2131, in particular the discussion of *ipsissimis verbis*. *Ipsissimis verbis* states that the elements of the invention must be arranged as required by the claim regardless of the identity of terminology. In other words, the fact that *Perlman* does not use the same terminology as the Applicant, yet teaches the elements of the claim language is not enough to distinguish the instant application over the prior art.

6. In response to the Applicant's arguments that *Perlman* does not disclose a proxy as a ending point for communication, the Examiner respectfully disagrees. As the Applicant has amended the claims, *Perlman* discloses receiving encrypted data at a proxy (i.e. firewall; figure 5 [block 506]) wherein the receiving completes a first hop and the proxy is an ending point of a fist communication associated with the first hop (i.e. Figure 5 [block 506]). *Perlman* discloses transmitting encrypted data to a firewall in a first communication as illustrated in at least figure 5 and below.

7. Therefore, *Perlman* discloses receiving encrypted data at a proxy wherein the receiving completes a first hop and the proxy is an ending point of a fist communication associated with the first hop and the rejection is maintained.

8. In response to the Applicant's arguments that *Perlman* does not disclose a proxy as a starting point for communication, the Examiner respectfully disagrees. As the Applicant has amended the claims, *Perlman* discloses sending the re-encrypted data from the proxy to an origin server (figure 5 [block 518]) over a given network wherein the sending starts a second hop and the origin server is an ending point of a second communication associated with the second hop. *Perlman* discloses transmitting encrypted data from a firewall to a server in a second communication as illustrated in at least figure 5 and below.

9. Therefore, *Perlman* discloses sending the re-encrypted data from the proxy to an origin server (figure 5 [block 518]) over a given network wherein the sending starts a second hop and the origin server is an ending point of a second communication associated with the second hop.

10. In response to the Applicant's argument that the firewall disclosed in *Perlman* is completely optional, the Applicant is reminded that the use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned and that they are part of the literature of the art relevant for all they contain. See MPEP § 2123; see *In re Heck*, 699 F.2d 1331, 1332-1333, 216 USPQ 1038, 1039 (Fed. Cir. 1983).

11. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as the client device being a wireless phone, are not recited in the rejected claim(s). Although the claims are

interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

12. See further rejections below.

Claim Rejections

13. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

14. Claims 1, 4-6, 8-10, 12-14, 16, 18-24, 26-28, 31, and 33-36 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,636,838 to Perlman et al., hereinafter Perlman.

15. As per claims 1 and 33, Perlman teaches a method comprising:

receiving encrypted data at a proxy from a client over an unsecure network wherein the receiving completes a first hop and the proxy is an ending point of a first communication associated with the first hop (Figures 4 [block 408], 5 [block 506], 10 [blocks 1006, 1008], column 5, lines 21-25, column 6, lines 1-2, column 6, lines 27-31, column 6, lines 51-61, column 9, lines 12-24);

decrypting the encrypted data into decrypted data (Figures 4 [block 412], 5 [block 514], 10 [block 1016], column 5, lines 21-25, column 6, lines 3-14, column 6, lines 32-39, column 6, line 62 to column 7, line 7, column 9, lines 29-31);

examining the decrypted data for security purposes (Figures 4 [block 414], 5 [block 516], 10 [block 1018], column 5, lines 26-32, column 6, lines 40-47, column 7, line 1-7, column 9, lines 32-36),

re-encrypting the examined decrypted data (column 5, lines 37-50); and

sending the re-encrypted data from the proxy to an origin server over a given network wherein the sending starts a second hop and the origin server is an ending point of a second communication associated with the second hop (Figure 5 [block 518], 10 [block 1020], column 5, lines 37-50, column 6, lines 48-50, column 7, lines 1-7, column 9, lines 34-36).

16. Regarding claim 4, Perlman teaches wherein the given network is a secure network (Figure 1 [block 109], column 4, lines 51-61).

17. With regards to claims 5 and 16, Perlman discloses wherein the sending is in accordance with one of the hypertext transport protocol (HTTP), the post office protocol (POP), the wireless access protocol (WAP), or the Internet messaging access protocol (IMAP) (column 4, lines 32-38, column 5, lines 51-67, i.e. wireless communications, "an e-mail message").

18. Regarding claim 6, Perlman teaches wherein the given network is one of the unsecure network and a second unsecure network (column 4, lines 51-61).

19. Regarding claims 8 and 19, Perlman teaches wherein the unsecure network is the Internet (Figure 1 [block 104], column 4, lines 32-39).

20. Regarding claims 9 and 24, Perlman teaches wherein the origin server is an effective origin server (column 4, lines 25-31).

21. Regarding claims 10 and 23, Perlman teaches wherein the client is an effective client (column 4, lines 25-31).

22. Regarding claims 12 and 26, Perlman teaches wherein the method is performed by a firewall within the given network (Figures 1 [block 106], 2 [block 106], 3 [block 106], 4, 5, 9 [blocks 106, 108], 10, column 4, line 20 to column 7, line 7).

23. Regarding claims 13 and 27, Perlman teaches a computer-readable medium having a computer program stored thereon for execution by a processor (column 4, lines 6-18, claims 3-4).

24. As per claim 14, Perlman teaches a proxy method comprising:

receiving unencrypted data from a client over an secure network (column 4, lines 32-37);

examining the unencrypted data for security purposes (Figures 4 [block 414], 5 [block 516], 10 [block 1018], column 4, lines 38-50, column 5, lines 26-32, column 6, lines 40-47, column 7, line 1-7, column 9, lines 32-36),

in response to the examining yielding that the unencrypted data does not present a security risk:

encrypting the unencrypted data into encrypted data (column 5, lines 37-50); and

sending the encrypted data to an origin server over an unsecure network (Figure 5 [block 518], 10 [block 1020], column 5, lines 37-50, column 6, lines 48-50, column 7, lines 1-7, column 9, lines 34-36).

25. Regarding claim 18, Perlman teaches wherein the secure network is a carrier network (column 4, lines 6-18).

26. Regarding claim 20, Perlman teaches wherein the client is a thin client (column 4, lines 25-31).

27. Regarding claim 21, Perlman teaches wherein the client is one of a: personal digital assistant (PDA) device, a laptop computer, a notebook computer, and a wireless phone (column 4, lines 25-31).

28. Regarding claim 22, Perlman teaches wherein the secure network is one of a wireless network or a wired network (column 4, lines 32-38).

29. As per claim 28, Perlman teaches a system comprising:

a client to send encrypted data over an unsecure network and be a starting point of a first hop (Figures 4 [block 408], 5 [block 506], 10 [blocks 1006, 1008], column 5, lines 21-25, column 6, lines 1-2, column 6, lines 27-31, column 6, lines 51-61, column 9, lines 12-24);

a proxy within a secure network to receive the encrypted data, decrypt the encrypted data into decrypted data, perform a test relative to the decrypted data, and send the decrypted data over the secure network in response to the test yielding a particular response wherein the proxy is an ending point of a first communication associated with the first hop and a starting point of a second communication associated with a second hop (Figures 4 [blocks 412, 414], 5 [blocks 514, 516], 10 [blocks 1016, 1018], column 5, lines 21-25, column 5, lines 37- 50, column 6, lines 3-14, column 6, lines 32-39, column 6, line 62 to column 7, line 7, column 9, lines 29-31); and,

an origin server within the secure network to receive the decrypted data and be an ending point of the second communication associated with the second hop (Figure 5 [block 518], 10 [block 1020], column 5, lines 37-50, column 6, lines 48-50, column 7, lines 1-7, column 9, lines 34-36).

30. As per claim 31, Perlman teaches a system comprising:

a client to send unencrypted data over a secure network (column 4, lines 32-37);

a proxy within the secure network to receive the unencrypted data, perform a test relative to the unencrypted data encrypt the unencrypted data into encrypted data, and send the encrypted data over an unsecure network in response to the test yielding a particular response (Figures 4 [blocks 412, 414], 5 [blocks 514, 516], 10 [blocks 1016, 1018], column 5, lines 21-25, column 5, lines 37- 50, column 6, lines 3-14, column 6, lines 32-39, column 6, line 62 to column 7, line 7, column 9, lines 29-31); and,

an origin server to receive the encrypted data (Figure 5 [block 518], 10 [block 1020], column 5, lines 37-50, column 6, lines 48-50, column 7, lines 1-7, column 9, lines 34-36).

31. Regarding claim 34, Perlman teaches wherein the first network is a secure network (column 4, lines 32-37).

32. Regarding claim 35, Perlman teaches wherein the second network is an unsecure network, such that sending the data to the origin server over the second network in the second hop comprises first encrypting the data (Figure 5 [block 518], 10 [block 1020], column 5, lines 37-50, column 6, lines 48-50, column 7, lines 1-7, column 9, lines 34-36).

33. Regarding claim 36, Perlman teaches wherein the second network is a secure network (column 4, lines 51-61).

34. Claims 7 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman in view of U.S. Patent No. 6,681,327 to Jardin, hereinafter Jardin.

35. Regarding claims 7 and 17, Perlman does not disclose wherein the receiving is within a secure socket layer (SSL) session.

36. Jardin teaches wherein the receiving is within a secure socket layer (SSL) session (column 1, lines 23-37).

37. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send the information over an SSL session, since Jardin states at column 1, line 38 to column 2, line 13 that such a modification would serve as authentication and encryption, thereby deterring hackers from eavesdropping and acquiring user information.

38. Claims 29, 30, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman.

39. Regarding claim 29, Perlman discloses a client within a secure network to send unencrypted data over the secure network; a proxy within the secure network to receive the unencrypted data, encrypt the unencrypted data into encrypted data, perform a test relative to the unencrypted data, and send the encrypted data over an unsecure network in response to the test yielding a particular response as seen in the rejections above.

40. Perlman does not disclose a second client and a second proxy.

41. It would have been obvious to one of ordinary skill in the art to include a second client and second proxy, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

42. Regarding claim 30, Perlman discloses a client to send second encrypted data over the unsecure network in an additional hop; a proxy to receive the encrypted data, decrypt the encrypted data into decrypted data, perform a test relative to the decrypted data, encrypt the decrypted data into encrypted data, and send the encrypted data over the unsecure network in response the test yielding a particular response as discussed above.

43. Perlman does not disclose a second client and a second proxy.

44. It would have been obvious to one of ordinary skill in the art to include a second client and second proxy, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

45. Regarding claim 32, Perlman discloses a proxy within a secure network to receive encrypted data, decrypt the encrypted data into decrypted data, and send the decrypted data over the secure network; and a origin server within the secure network to receive the decrypted data as illustrated above.

46. Perlman does not disclose a second proxy or a second origin server.

47. It would have been obvious to one of ordinary skill in the art to include a second proxy and a second server, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

Conclusion

48. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

49. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR

1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

50. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Thursday 7-5.

51. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

52. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

CHRISTOPHER REVAK
PRIMARY EXAMINER

8/31/06